

Aventures de voyage aux conséquences désagréables

Pour plus de sécurité, adoptez les réflexes CASES !

...et comment les éviter

Internet est devenu incontournable pour beaucoup d'entre-nous, même en vacances ou pendant de courtes escapades. Une chose est pourtant dommage, voire même tragique : entièrement tournés vers la détente et le plaisir, les voyageurs ont toutes leurs antennes en vacances. La sécurité est vite oubliée.

Tout le monde parle de vacances et les Luxembourgeois ne font pas exception. Certains ont réservé leur vol ou leur hôtel via Internet. D'autres ont préparé leur itinéraire en ligne à la maison. Et à destination ? Que font-ils ?

Un collaborateur de CASES, le portail luxembourgeois de la sécurité de l'information, a sondé les voyageurs cette semaine à l'aéroport de Luxembourg. Voici les résultats : « Ne faire que se baigner, c'est ennuyeux. Je veux garder le contact avec mes amis via Facebook et Twitter » ; « Nous enverrons les plus belles photos de vacances directement à la maison » ; « Je voyage



malheureusement avec mon ordinateur portable pour lire mes e-mails professionnels et y répondre » ; « Nous irons dans un cybercafé pour réserver une voiture de location » ; « Nous ferons beaucoup de choses en ligne : réserver une table au restaurant, gérer le portefeuille d'actions et dénicher des conseils d'excursion à proximité » ; « En vacances, je me limite à verser mon loyer et, grâce à Internet, c'est aussi possible depuis l'hôtel ».

Il faut souligner une chose : cela casse certes l'ambiance des vacances estivales, mais les voyageurs qui utilisent les nombreuses possibilités de la technique numérique à

destination peuvent tomber dans des pièges de sécurité s'ils oublient les réflexes de protection nécessaires !

Pourquoi courir un risque justement à la plus belle période de l'année ? Premièrement : dans une ambiance décontractée, libérés du quotidien, beaucoup de gens mettent les préoccupations de sécurité sur le côté et oublient soudainement les mesures de protection les plus élémentaires. Deuxièmement : même dans les plus beaux endroits de la planète, personne n'est malheureusement à l'abri de méfaits. Les lieux touristiques sont aussi le terrain d'action



privilegié des voleurs et cybercriminels.

Les 8 A pour plus de sécurité en vacances

Comment les vacanciers devraient-ils se comporter avec les ordinateurs, Internet, téléphones mobiles, etc. ? Les 8 A des réflexes de sécurité peuvent vous aider.

ABSENCES : ne pas les annoncer. Il est incroyable de voir le nombre de personnes qui annoncent leurs projets de voyage et même leur itinéraire sur Internet. Que ce soit par blog, sur les réseaux sociaux comme Facebook et Twitter ou sur leur site web personnel. Le problème ? Grâce à ces informations, les cambrioleurs peuvent découvrir si et quand les résidents d'une maison ou d'un appartement sont en vacances. Le cambriolage peut ensuite se faire tranquillement.

Mesure de protection : les voyageurs doivent vérifier s'il y a sur leur site web, leur blog ou leurs réseaux sociaux des données personnelles qui pourraient indiquer aux voleurs que leur logement est inoccupé. Les réponses automatiques par e-mail et répondeurs téléphoniques ne doivent pas non plus fournir trop de détails.

ANTIVIRUS, etc. pour l'ordinateur portable.

Conseil de sécurité : effacer les traces dans les cybercafés

Les plus curieux peuvent découvrir les adresses Internet consultées par les voyageurs. L'historique (History), la mémoire cache (mémoire tampon, fichiers Internet temporaires) et les cookies renseignent sur la session Internet du voyageur. CAGES conseille de supprimer toutes les traces de surf sur les ordinateurs publics. Les voyageurs sont invités à s'exercer à supprimer les données à la maison parce que les textes de commande apparaissent souvent dans la langue nationale à l'étranger. **Supprimer les données dans Internet Explorer :** avec le bouton gauche de la souris, cliquez sur le bouton « Outils » dans le coin supérieur droit de l'écran et sélectionnez l'entrée « Supprimer l'historique de navigation ». Vous pouvez alors choisir ce que vous voulez effacer : les fichiers Internet temporaires, les cookies, l'historique, les mots de passe, etc. **Supprimer des données dans Firefox :** pour effacer la mémoire cache en même temps que les termes recherchés, ouvrez le point « Outils » dans la barre de menu. Choisissez alors « Paramètres » suivi de « Protection des données ». Veillez à ce que les sites visités ne soient pas enregistrés et à ce que l'historique soit supprimé quand vous quittez Firefox. Allez sur « Paramètres » pour déterminer les données qui doivent être supprimées automatiquement, par exemple « Sites visités », « Chronique de téléchargement », « Termes recherchés saisis & données de formulaires », « Cookies », « Logins actifs », « Cache » et « Mots de passe enregistrés ». N'oubliez pas de confirmer vos paramètres avec « OK ». Vous pouvez vérifier si l'historique des sites web fréquentés a été réellement effacé. Pour cela, appuyez sur les touches [ctrl] et [H] – pour ouvrir sur la gauche de l'écran une colonne reprenant toutes les entrées de l'historique. Il ne doit plus y avoir aucune entrée.

Définition : mini-support de données

Il s'agit des clés USB ou des cartes de mémoire des appareils photos. Si des données personnelles sont enregistrées sur ces supports de données, leur utilisation par un tiers ne peut être exclue en cas de perte du support. Par ailleurs : les supports de données et cartes de mémoire peuvent aussi être contaminés par des logiciels malveillants. Cela peut, par exemple, arriver dans un magasin photo utilisant des ordinateurs non protégés. Une mauvaise surprise attend ensuite le voyageur lors de la prochaine utilisation.

Nombre de voyageurs ne peuvent ou ne veulent pas renoncer à leur ordinateur portable même en vacances. L'ordinateur permet de consulter les e-mails et de communiquer avec les amis et proches. Les voyageurs sont bien inspirés de vérifier

que les programmes de l'ordinateur portable, notamment l'antivirus, sont mis à jour et que le firewall est bien configuré. Pour éviter toute utilisation non autorisée de l'ordinateur portable, les voyageurs doivent protéger l'ouverture

de session par un mot de passe.

Si le vacancier emporte son ordinateur, il doit aussi s'assurer que les données sensibles sont protégées des accès étrangers par cryptage. Il évitera ainsi que des données sensibles tombent entre les mains de tiers en cas de vol. Il ne faut en outre jamais laisser l'ordinateur portable sans surveillance, que ce soit à l'hôtel ou au restaurant, dans le train ou même dans la voiture. Cette précaution évite le vol par occasion.

AVOIR L'OEIL sur les tentatives d'espionnage. Un avertissement contre l'espionnage sur le lieu de villégiature ? Ce n'est malheureusement pas une fiction mais peut être la réalité d'un vacancier. Cela concerne essentiellement les ordinateurs en libre accès dans les cybercafés et hôtels. Le problème ? Avec les ordinateurs publics, il y a toujours un risque que les criminels exploitent les failles de sécurité et installent des logiciels malveillants de façon ciblée ou se servent des faiblesses dans le comportement des utilisateurs. Des mots de passe, données bancaires ou commerciales ou d'autres informations personnelles peuvent ainsi tomber entre les mains de personnes malintentionnées.

D'autres formes « d'espionnage » sont plutôt

banales mais non moins dangereuses : il se peut par exemple qu'une caméra de surveillance soit orientée vers l'écran et le clavier du vacancier. Les escrocs n'hésitent pas non plus à regarder au-dessus de l'épaule des vacanciers ou à se promener près des ordinateurs pour dérober des informations.

Mesure de protection : les voyageurs doivent si possible toujours se placer dans un coin ou avec le dos au mur. Ils ne doivent en aucun cas s'éloigner de leur ordinateur public s'ils consultent des sites Internet sensibles, même pour de courtes pauses. Ils peuvent éventuellement identifier un logiciel-espion si l'ordinateur est bizarrement lent lorsqu'ils surfent sur Internet.

APPLICATIONS comme l'e-banking à éviter à tout prix. Régler ses affaires bancaires sur un ordinateur public, entre l'hôtel et la piscine ? Plutôt pas ! Le risque de divulguer des mots de passe à cause d'un logiciel-espion ou d'une connexion non sécurisée est trop important. Même chose pour les achats et la réservation « en ligne et par carte de crédit ». Mesure de protection : il est préférable de renoncer à tout type de transaction en ligne sur des ordinateurs publics.

Les virements urgents éventuels doivent être confiés à une banque locale. S'il est impossible d'éviter les

activités de commerce électronique, il est conseillé aux voyageurs de vérifier si l'ordinateur est sûr. Les vacanciers doivent en outre toujours saisir les adresses Internet manuellement, ne pas cliquer sur des liens dans des e-mails, veiller à la transmission cryptée de leurs données et imprimer les informations de commande et les e-mails importants.

ARRÊTER LA CONNEXION et supprimer toutes les données privées. Un internaute laisse toujours des traces de ses activités sur l'ordinateur. Les voyageurs ne doivent pas l'oublier. Des informations telles que les sites web visités ou les renseignements fournis dans des formulaires peuvent aider un pirate à s'approprier le profil d'un vacancier. Le cybercriminel peut alors se connecter sur des sites web avec authentification (webmail, e-commerce, e-banking) grâce à ces données.

Mesure de protection : il est conseillé aux vacanciers de supprimer toutes les traces laissées sur un ordinateur public après une session de surf et de ne jamais y enregistrer de mots de passe. Les sessions et applications doivent toujours être fermées correctement, c'est-à-dire via « Quitter », « Terminer », « Logout » ou toute autre fonction similaire. Beaucoup d'utilisateurs font l'erreur de cliquer sur la croix pour fermer la fenêtre du

navigateur croyant ainsi que leur connexion est coupée. Ce n'est pas le cas. Un tiers peut rouvrir la fenêtre et accéder à la connexion encore ouverte.

Les criminels peuvent intercepter des données

ATTENTION avec les accès sans fil. Les lieux de connexion Internet dans les hôtels, gares, aéroports, restaurants ou cafés sont pratiques mais pas toujours fiables. Ils sont souvent appelés « Hotspot », « WLAN », « WiFi » ou « réseaux mobiles » et permettent de surfer sans fil.

Le problème ? Les personnes qui se connectent ici doivent s'assurer via l'exploitant que le point de connexion répond au moins aux normes de sécurité minimales comme la visibilité claire du nom du point de connexion. Habituellement, il n'est pas possible pour l'utilisateur de reconnaître si les principales mesures de sécurité sont garanties par l'exploitant. Les criminels sont très rusés et installent leurs propres réseaux privés à proximité des points de connexion publics. Le but est d'intercepter des connexions de clients pour lire les données et informations confidentielles.

Le portail de la sécurité de l'information CASES du Ministère de l'Économie et du

Commerce extérieur a établi des normes de sécurité minimales pour les points de connexion.

Les établissements luxembourgeois qui proposent de tels points répondant à ces normes peuvent obtenir rapidement, facilement et gratuitement un label renouvelable annuellement. Les utilisateurs ont ainsi une aide pour s'informer sur la sécurité de tels accès Internet.

ATTENTION aux enfants. Les enfants veulent surfer dans un cybercafé ou sur l'ordinateur de l'hôtel pendant leurs vacances ? Une des règles fondamentales : les vacanciers ne doivent jamais laisser leur enfant sans surveillance, même sur l'ordinateur. Les enfants doivent être avertis qu'ils ne doivent jamais transmettre à des tiers ni publier des informations personnelles telles que des adresses, des numéros de téléphone, le lieu de résidence, l'école, les projets de vacances, etc. Les criminels sont friands de ces informations.

Les parents doivent garder un œil sur leur enfant lorsqu'ils téléchargent des jeux, des vidéos ou des fichiers musicaux pour éviter les frais imprévus. Cela vaut tout spécialement pour les téléphones mobiles. Les enfants ne doivent pas non plus envoyer des photos de vacances actuelles sur des

plateformes sans connaître les paramètres de sécurité nécessaires. Ici, les parents peuvent donner le bon exemple en s'abstenant de publier sur Internet des photos que des millions d'utilisateurs pourront voir.

À GARDER À L'ESPRIT : les voleurs classiques. Ne pas oublier : il y a aussi des vols classiques pendant les vacances. Quelques secondes d'inattention et le voleur a disparu dans la foule. Le problème ? D'une part, le vol ou la perte d'ordinateurs portables ou de téléphones mobiles occasionne des dommages matériels. D'autre part, un tel vol ou une telle perte peut aboutir à la perte définitive ou au détournement des données privées précieuses qui se trouvent sur ces appareils.

Mesure de protection : les voyageurs ne doivent emporter en vacances que les appareils dont ils ont réellement besoin. À destination, ils ne doivent jamais les laisser sans surveillance. Même les mini-supports de données comme les clés USB doivent être à l'abri. Or, ils sont très faciles à oublier dans un cybercafé. Il est conseillé aux voyageurs d'effacer toutes les informations privées et professionnelles se trouvant sur les clés USB avant de prendre le départ.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu